FORUM SYSTEMS™

THE LEADER IN WEB SERVICES SECURITY

FORUM SYSTEMS SENTRY™ VERSION 8.1
GUIDE TO SECURITY WORLDS

Legal Marks

Forum Systems Sentry™ Version 8.1 Guide to Security Worlds, published January, 2013.

D-ASF-SE-01788

Table of Contents

List of Figures

INTRODUCTION TO THE GUIDE TO SECURITY WORLDS

Audience for the Guide to Security Worlds

The *Forum Systems Sentry™ Version 8.1 Guide to Security Worlds* provides a step-by-step guide for managing Security World Keys. The goal of the *Forum Systems Sentry™ Version 8.1 Guide to Security Worlds* is twofold:

- to explain the concept of a Security World within the context of the Forum Systems XML Security System™ as it pertains to the embedded FIPS 140-2 Level III HSM Module.
- to enable effective management of Security World keys.

Conventions Used

A red asterisk (*) aligned with a field term means that this field is required.

In this and other documentation, the Web Administration Interface is referred to as the WebAdmin and the Forum XML Security Appliance™ is referred to as the 'device', 'product' or 'system'.

In this document, all data or commands that must be entered or selected are displayed in boldface. Example:

User name:	johnsmith
Password:	********

UI screens which display a STATUS column represent the following states:

- Green status light = enabled policy.
- Yellow status light = a required functional element of this policy is disabled.
- Red status light = disabled policy.

Throughout this and other documents in the Documentation Set, repetitive actions such as:

- View / edit a policy.
- Enable / disable a policy.
- Delete a policy.
- Rename a policy.
- Limit display of policies with Search or Max Results fields.

are not shown. For more information, refer to the Common Operations section of the *Forum Systems Sentry™ Version 8.1 Web-based Administration Guide*.

Customers with plug-in licenses on the system, confirm that your Integration License is visible on the General Info screen under the SUPPORTED FEATURES section.

Any specifications and constraints referenced in this volume appear in the Appendices of this volume.

What is a Security World

Every Forum Sentry FIPS 140-2 Level III HSM operates within a context known as a “Security World.” Each Security World has a unique secret key that protects any application keys created (or imported) by an administrator on the system. Only an HSM which has been initialized with a particular Security World can understand application key-data created by an HSM in that Security World. Therefore, in order for multiple HSM enabled systems to share key-data, each system’s HSM must be initialized in the same Security World context.

Note: The Security World key is important in that different HSM-enabled systems can only share configurations if their HSM module is initialized with the same Security World key. For more information, refer to the Import a Configuration from an HSM-enabled System to Another HSM-enabled System chapter.

PREPARE FOR INSTALLING THE PRODUCT

Note: When the HSM-enabled system is first installed, the HSM must be initialized with a Security World. What follows is a brief description of the installation procedure focusing on the HSM initialization. For a more in-depth discussion of the installation procedure, refer to the *Forum Systems Sentry™ Version 8.1 HSM Quick Start Guide*.

Installation Overview

The following is an overview of installation steps, presented in sequence, to install the product:

- Decide on in-line or 1-port physical network configuration for the product.
- Setup the serial port console cable connections to the product.
- Initialize the system via the Command Line Interface (CLI) (start terminal emulation software, e.g. Hyper Terminal™, and connect to product).
- The Forum Systems Installation Wizard appears and prompts you to initialize the HSM with a Security World, configure Network Interfaces for the product, the WebAdmin UI, and add the first Listener Network policy and first product user.
- Add additional product users, if desired.
- At this point in the installation sequence, Administrators would add listeners by creating Listener Network policies.

Note: If you would like to initialize the HSM with an existing Security World, you will need to have a bootstrap file from another HSM-based system that has been initialized with the desired Security World available, along with an Administrator card and the password for that Administrator card for that system.

Requirements for Forum Systems Installation Wizard

After physically installing the product and connecting to the CLI, follow the Forum Systems Installation Wizard to configure the product.

The Installation Wizard requests the following items:

1. IP address and netmask for the Management Port for the product.

2. IP address and netmask for the device port(s) of the product.

3. Default Device Gateway for the product.

4. Primary and/or Secondary DNS Server IP addresses (optional).

5. The network configuration options for your servers are: 1-port mode, In-line mode (Single IP address) and In-line mode (Dual IP addresses). Before physical installation, IT Administrators must decide which mode best matches your network structure:

   - With 1-port mode configuration, the product operates using a single network interface connected to the corporate network. Client requests will be directed to the IP of the product.
   - With in-line mode (Single IP address) configuration, the product sits between the corporate "Local Area Network" and the outside "Wide Area Network" with two network interfaces being used for bi-directional network traffic. In-line mode configuration means the product sits between client and back end servers.
   - With in-line mode (Dual IP address) configuration, the system is configured in In-line mode with a LAN IP address and LAN netmask as well as a WAN IP address and WAN netmask.

6. Decide on the Enable mode password.

7. Decide on the WebAdmin user name and password.

8. If installing an HSM-enabled system, gather your Card Reader and Administrator cards.

System Schematic for the FIPS 140-2 Level III HSM-enabled System

The following diagram displays the FIPS 140-2 Level III HSM-enabled System:

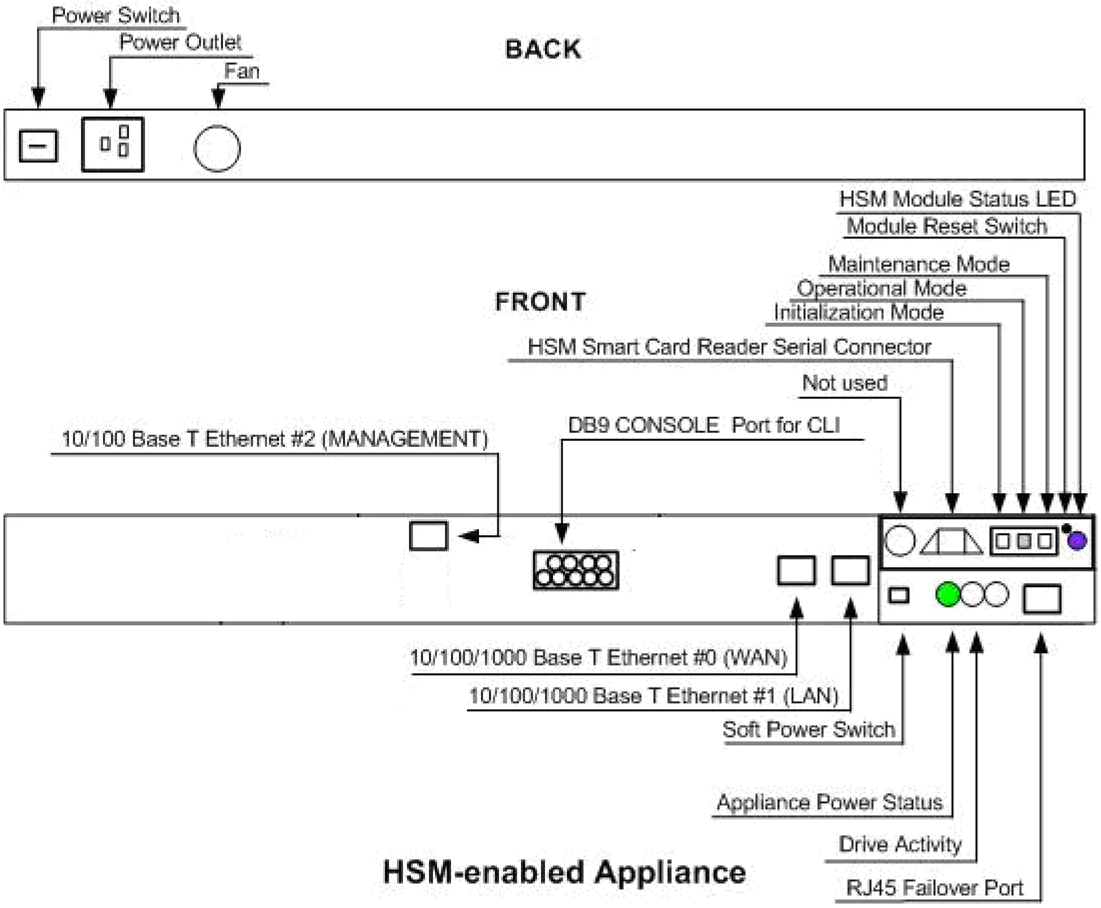


Figure 1: Product Schematic for the FIPS 140-2 Level III HSM-enabled System.

INITIALIZE HSM ON AN HSM-ENABLED SYSTEM FOR THE FIRST TIME

The Hardware Security Module

Note: As part of the installation procedure, the HSM module must be initialized with a Security World key which will protect all of the application keys which are later generated for use within the system.

HSM Modes on the Product

The HSM operates in three modes, visible at the front of the system:

- Initialization mode is used exclusively when first initializing (or re-initializing) the HSM module for normal operation.
- Operational mode is used during normal operation.

Note: The mode switch should always be left in this position by default. Should an operation in the CLI or product require you to move the switch, it will prompt you to do so. If the switch is not n this position when the product boots, the product may fail to initialize properly.

- Maintenance mode is used exclusively for upgrading the module's firmware.

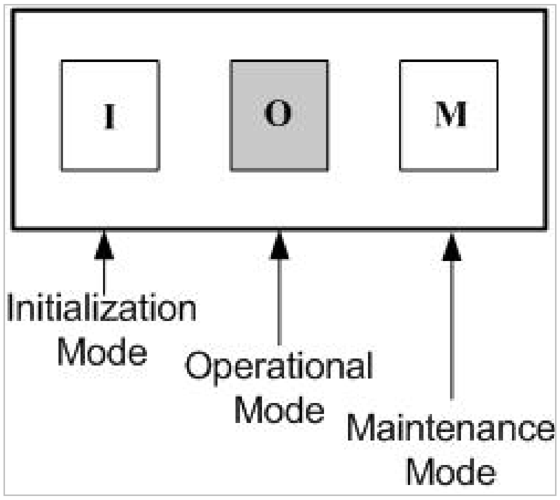


Figure 2: HSM Modes on the HSM-enabled System.

Learn About HSM-related Keys

HSM-enabled products use a hierarchical protection scheme for private keys stored on the product.

Application Keys

At the lowest level are the application keys. These are the keys that the user loads onto the product for such uses as encryption/decryption or signing/signature-verification. Once loaded onto the product through the standard means (*i.e. through key generation, key import, or configuration import*), these keys are protected by the HSM. The HSM encrypts these keys using the ***Security World Key*** and stores the encrypted values on the product's backing store.

When these application keys are referenced by the system, if they are not already loaded onto the HSM, the HSM loads them and decrypts them (internally, on the tamper proof module) using the security world key so that they may be used for cryptographic operations on the system.

Security World Key

The Security World Key is the key with which the HSM is originally initialized. It, too, has an encrypted backup version stored on the product's backing-store. When the HSM module is initialized, that encrypted version is loaded and decrypted (again, internally on the tamper proof module) so that it may be used to decrypt the application keys when they are loaded onto the module. This decrypted Security World Key will remain on the module until the next time the module is initialized. The encrypted, stored version of the Security World Key is encrypted with a key stored on an Administrator card at the time when the Security World Key is generated (usually, this is done as part of the HSM initialization process).

Administrator Cards

The keys stored on Administrator cards are encrypted using a passphrase which is set by the user when the Administrator card is first initialized. The Administrator cards are initialized as part of the process that creates a new Security World Key (a new Security World Key is usually created as part of the HSM module initialization process).

If an HSM is to be initialized with an existing Security World Key (as opposed to with a newly generated Security World Key), the user must be prepared to submit a corresponding Administrator card and its passphrase to the initialization sequence in order to load the encrypted version of the existing Security World Key onto the module.

Types of Keys

A summary of the types of keys follows:

TYPE OF KEY	DESCRIPTION
Application keys	These are the user's keys (including private/secret keys) used in encryption/decryption and signing/signature-verification policies on the product. They are stored, encrypted by the security world key, on the product's backing store and are loaded onto the module and decrypted when needed.
Security World Keys	Each HSM module is loaded with a Security World Key. The HSM module uses this key to protect (encrypt) all application keys loaded onto a product. A version of this key is stored encrypted, by an Administrator card key, on the product's backing store.
Administrator card keys	Administrator card keys are generated at the same time as a new Security World Key. The Administrator card keys are used to encrypt the Security World Key stored on the product's backing store. The Administrator card keys are each encrypted with a user supplied passphrase and stored on an Administrator card.
Administrator card passphrases	HSM Administrator card passphrases are used to protect Administrator card keys. They are case sensitive and must be unique, from 6 to 128 alphanumeric characters, and may include underscores, dashes, and spaces. However, leading and trailing whites pace is ignored.

For information about importing configurations with HSM-enabled keys, refer to the Import / Export chapter of the *Forum Systems Sentry™ Version 8.1 System Management Guide*.

Attach the HSM Card Reader

Initializing the HSM module requires use of the provided HSM card reader. Follow these steps to install the HSM card reader of the HSM-enabled System:

- If not already attached, attach the Electro Magnetic Interference (EMI) filter (adapter) on to the front of the product. Refer to the HSM Modes on the HSM-enabled System section).
- Attach the free end of the card reader's serial connector to the EMI filter.

Note: The smart card reader LED status is now red, indicating that the Smart card reader is powered.

Learn about Security World Keys

The FIPS 140-2 Level III HSM-enabled product has a concept of a "Security World" and a "Security World" key. This means that all of the application keys which are stored on the product are encrypted using the same Security World Key.

An encrypted version of this key is also stored on the product – it is encrypted using a key on the Administrator cards. The keys on the Administrator cards are also encrypted using a passphrase that is supplied when the Security World Key and Administrator card key are generated. To enable HSM, the module must be initialized with a Security World Key (a procedure that requires the encrypted Security World Key, an Administrator card, and its passphrase). Only keys created in the Security World in which the module is currently initialized are available for use in the system.

When the product is booted for the first time (or after running the CLI command ***system config factory-reset***), the first part of the Forum Systems Installation Wizard walks the user through initialization of the HSM module.

The first option offers the choice of initializing the HSM with an existing Security World or a newly generated one. Selecting to use an existing Security World will prompt to upload a bootstrap file (refer to the "management bootstrap export" command in the *Forum Systems Sentry™ Version 8.1 Command Line Interface Reference*) containing the Security World information and will require an Administrator card for that security world and its passphrase.

```
*******************************************************
*           HSM Settings for the System            *
*                                                     *
* This section will help you set up your Hardware     *
* Security Module.  You will need the card reader     *
* and smart cards that came with your system.      *
* NOTE: The system may take a few moments to complete *
* some of the operations necessary to initialize the  *
* HSM module.                                         *
*******************************************************

# The HSM module must be initialized with a security world key
# Would you like to initialize the module with:
  1. A newly generated security world key and Administrator Cards
  2. A security world key from a bootstrap file using a corresponding
Administrator Card

> 2 <enter>
[Select 2 to load an existing security world's information from a bootstrap
file using a corresponding Administrator card, and then press <enter>]
```

```
Ready to receive file via zmodem...
Š□B000000023be50

[Initiate zmodem file upload from terminal emulation software]

# Please set the switch on the HSM module to "I" and press enter

> <enter>
[Set the switch on the HSM module to “I”, and then press <enter>.]


# Please insert an Administrator card (1/1) to be loaded and press enter.

> <enter>
[Insert the Administrator Card into the Smart Card Reader, and then
press <enter>.]

# Please enter: a passphrase
# The passphrase for the current Administrator Card

******* <enter>
[Enter the passphrase for the current Administrator card, and then
press <enter>.]


# To complete HSM initialization, please set the switch on the HSM module
# to "O" and press enter

> <enter>
[Set the switch on the HSM module to “O”, and then press <enter>.]


# Please enter: Data entry method
# Manual enter data or import an existing bootstrap file
  1 to manually enter data
  2 to import a bootstrap (fsb) file
  3 to use the existing imported bootstrap (fsb) file

> 3 <enter>
[Type 3, and then press <enter>.]


Installation Wizard is now complete!

Logged into Command mode
Type ? for a list of commands

ForumOS>
```

Initializing HSM Examples

Examples for Initializing HSM include:

- Initialize HSM with A Newly Generated Security World.
- Initialize HSM with a New Security World Key.

Initialize HSM with a Newly Generated Security World

The following section discusses how to initialize an HSM with a newly generated Security World.

The Administrator will be prompted for the number of Administrator cards to generate. Typical initialization process follows these steps:

- Set switch on HSM module to “I” mode.
- Insert Administrator card into the smart card reader, and the smart card reader LED turns green.

Note: The metallic strip on smart card should be inserted first, face up.

- Provide passphrase for Administrator card.
- Repeat steps 2 and 3 for all Administrator cards to be generated.
- Set switch on HSM back to “O” mode.

Note: Should the user ever wish to transfer key data from this product to another HSM-enabled product, you will need an Administrator card (and its passphrase) produced in this procedure. For more information, refer to the GDM Full Configuration Imports chapter of the *Forum Systems Sentry™ Version 8.1 System Management Guide.*

Initialize HSM with a New Security World Key

The Forum Systems Installation Wizard will prompt users to initialize the HSM and enter Administrator cards and passphrases to enable Hardware Key Management on the product with a new Security World Key. The following operation demonstrates initializing the HSM using a single Administrator card. However, users may initialize more Administrator cards if desired.

Note: Forum Systems strongly recommends initializing multiple Administrator cards for the machines which will be configured in the new Security World. Once the set of Administrator cards is created, the number of cards in the set can not be changed.

The module switch should always be set to “O” mode unless you are initializing the module. Problems may arise when the product is booted up and the module switch is not set to “O” mode; the product may not load properly.

The Forum Systems Installation Wizard displays the following start-up screen and sequenced prompts:

```
*******************************************************
*  Welcome to the Forum Systems Installation Wizard   *
*                                                     *
* Before using the command line interface, some       *
* basic information will be needed to configure       *
* the management network interface and the hardware   *
* security module (HSM).  Type exit at                *
* the command prompt if you would like to defer       *
* this wizard until later.                            *
*                                                     *
* Once this information is collected, you will be     *
* able to use the command line interface or the       *
* the WebAdmin gui.                                   *
*                                                     *
*******************************************************

*******************************************************
*           HSM Settings for the System            *
*                                                     *
* This section will help you set up your Hardware     *
* Security Module.  You will need the card reader     *
* and smart cards that came with your System.     *
* NOTE: The system may take a few moments to complete *
* some of the operations necessary to initialize the  *
* HSM module.                                         *
*******************************************************

# Please enter: number of Administrator Cards
# The number of Administrator Cards to create for this Security World.
> 1 <enter>

# Please set the switch on the HSM module to "I" and press enter.
> <enter>
[Physically switch the Mode of the HSM module to I (Initialization) at the
front of the product, and then press <enter>.]
```

Note: Refer to Product Schematic for the HSM-enabled System and the HSM Modes on the HSM-enabled and System sections for detailed view of HSM modes on the front of the product.

```
# Please insert an Administrator Card (1/1) to be initialized and
# press enter.
>  <enter>
[Insert the first Administrator Card into the Smart Card Reader, and then
press <enter>.]
```

Note: Insert Administrator cards into the smart card reader with the copper strip facing up (toward the ceiling). The LED status is now green, indicating that a smart card is properly seated in the smart card reader.

```
# Please enter: a passphrase
# A new passphrase for the current Administrator Card
# (The passphrase length should be between 6 and 128 characters.
# Leading and trailing whitespace will be ignored.)
> ******** <enter>
[Enter Passphrase, and then press <enter>.]
```

Note: The command line will not echo "*" characters.

```
# Please enter: a passphrase
# Please confirm the passphrase for the current Administrator Card.
> ******** <enter>
[Re-enter Passphrase, and then press <enter>.]
```

Note: The command line will not echo "*" characters.

```
# To complete HSM initialization,   please set the switch on the HSM module
# to "O" and press enter.
> <enter>
[Physically switch the Mode of the HSM module to O (Operational) at the front
of the product, and then press <enter>.]
```

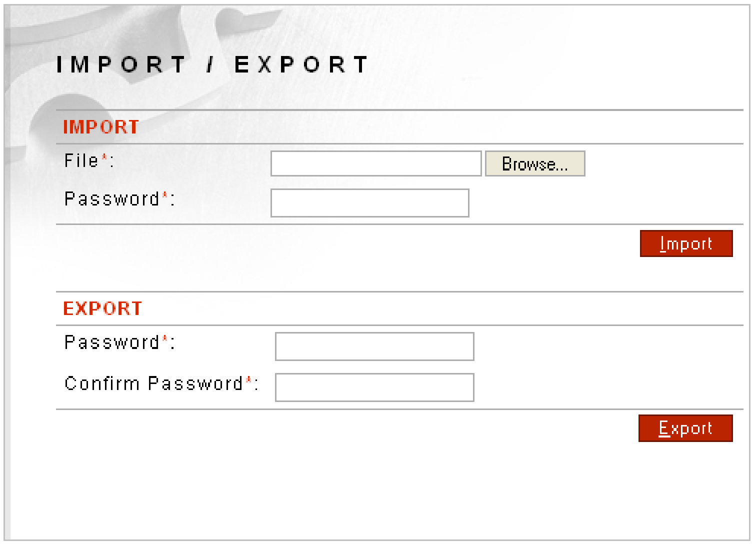
Note: For the remainder of the installation procedure, refer to the *Forum Systems Sentry™ Version 8.1 HSM Quick Start Guide*.

IMPORT OR EXPORT CONFIGURATION FROM THE PRODUCT

Import or Export Overview

This system provides a method for importing and exporting system configuration information, including policies, device setup, namespace and key data on the Import / Export screen. On an HSM enabled platform, transferring Security Worlds between HSM-enabled systems is part of the configuration import/export procedure.

The Import / Export screen provides a means of exporting system configuration information to import to other systems (for duplication or upgrade purposes) and also allows users to back up configuration information from their systems.



The operations available on the Import / Export screen include:

- Export System configuration.
- Import System configuration.

Only one configuration may be active on the system at one time. Importing a new configuration file (i.e. <filename>.fsx) will override the currently active configuration file. Exporting a configuration file will export a copy of the system's complete configuration information to a file. Configuration files are automatically named after the export date; i.e., config082903.fsx, and can be renamed prior to saving.

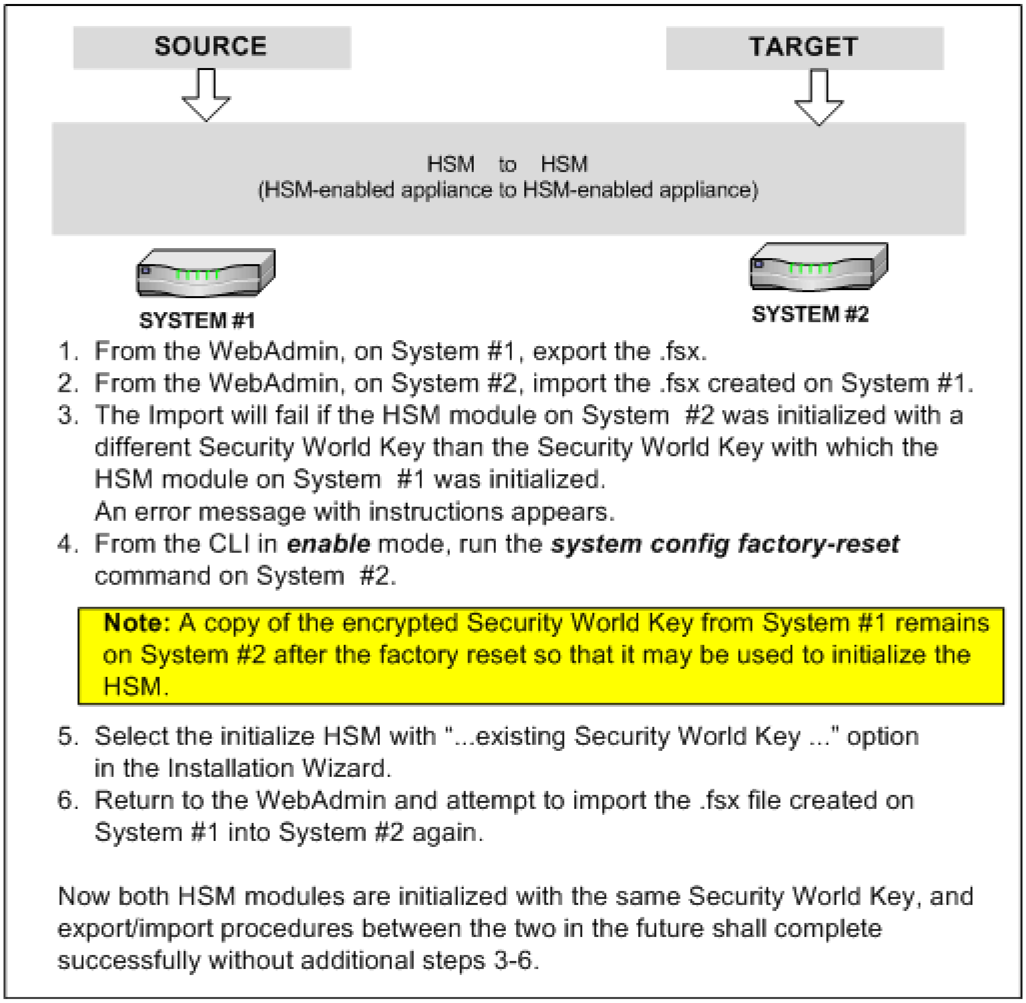
Network information (the management IP, the device IP, default gateway, primary DNS, secondary DNS, NTP server, and other associated settings) are not passed along with the fsx file. Whichever system you import into will retain its original network information (the management IP, the device IP, default gateway, primary DNS, secondary DNS, NTP server, and other associated settings).

Import or Export Password

The password entered during the Import configuration operation or export configuration operation is bound to that file. When exporting a file, the password provided is used to encrypt the .fsx file. Only by entering the same ***password*** while importing the .fsx file will the import process be successful.

Import or Export Configurations with Various System Versions

The following graphic displays an overview of HSM-enabled Systems for exporting / importing configuration files (.fsx) between two HSM-enabled systems:



1. From the WebAdmin, on System #1, export the .fsx.
2. From the WebAdmin, on System #2, import the .fsx created on System #1.
3. The Import will fail if the HSM module on System #2 was initialized with a different Security World Key than the Security World Key with which the HSM module on System #1 was initialized.
   An error message with instructions appears.
4. From the CLI in ***enable*** mode, run the ***system config factory-reset*** command on System #2.

> **Note:** A copy of the encrypted Security World Key from System #1 remains on System #2 after the factory reset so that it may be used to initialize the HSM.

5. Select the initialize HSM with "...existing Security World Key ..." option in the Installation Wizard.
6. Return to the WebAdmin and attempt to import the .fsx file created on System #1 into System #2 again.

Now both HSM modules are initialized with the same Security World Key, and export/import procedures between the two in the future shall complete successfully without additional steps 3-6.

Figure 3: Import or Export Configurations with Multiple Systems.

The system supports importing configurations created on other systems up to one major version release behind the target system version.

> **Note:** When working on the system with Version 5.1.234 of the software, for example, Administrators may import any configuration version between 4.0.0 and 5.1.234. Likewise, Version 6.3.789 will be able to import any configuration between 5.0.0 and 6.3.789. Any exported configuration file built more than one major version prior will fail to import into the system.

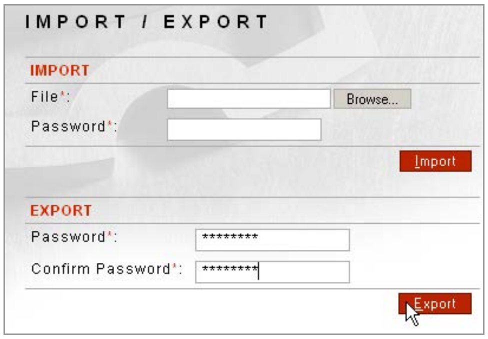
Import and Export Configuration Examples

Examples for Import and Export Configurations include:

- Export System Configuration.
- Import Same Configuration from an HSM-enabled System to Another.
- Import Existing Configuration from an HSM-enabled System to Another Initialized with Different Security World Key.

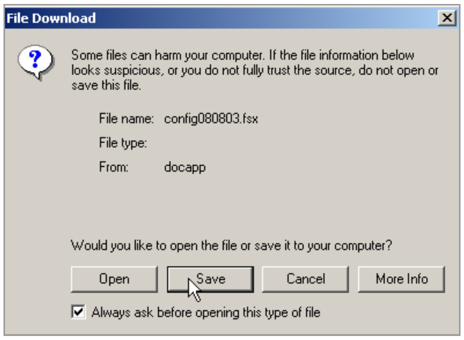
Export System Configuration

Exporting a configuration will result in a configuration file being generated and encrypted with the password that you supplied. Later, when you want to import this file, enter the same password in the IMPORT Password field to decrypt the file and import the configuration.



Password*: ********

Confirm Password*: ********



Some files can harm your computer. If the file information below looks suspicious, or you do not fully trust the source, do not open or save this file.

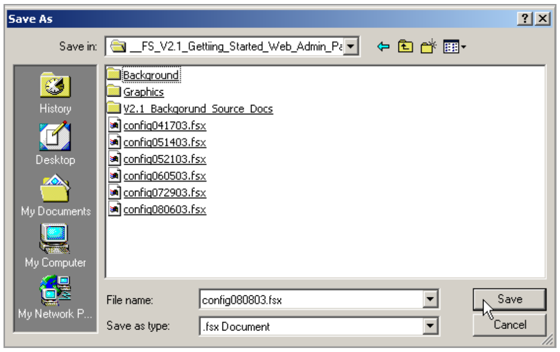
File name: config080803.fsx

File type:

From: docapp

Would you like to open the file or save it to your computer?

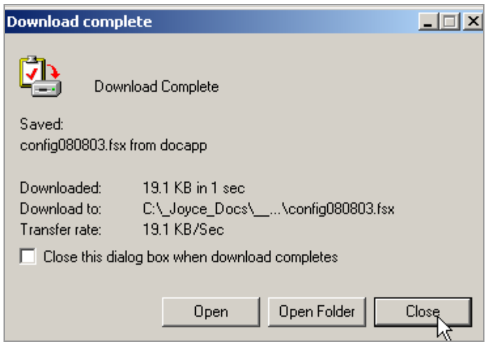
☑ Always ask before opening this type of file



Save in: __FS_V2.1_Gettiing_Started_Web_Admin_Pa

File name: config080803.fsx

Save as type: .fsx Document



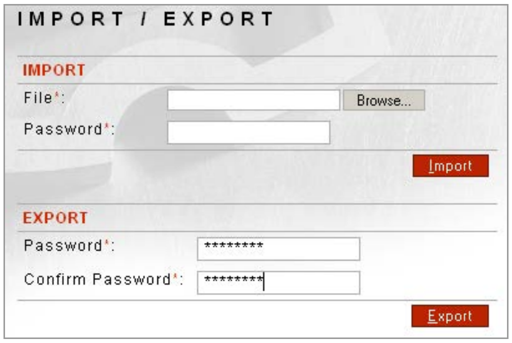
Download complete

Download Complete

Saved:
config080803.fsx from docapp

Downloaded: 19.1 KB in 1 sec
Download to: C:_Joyce_Docs__...\config080803.fsx
Transfer rate: 19.1 KB/Sec

□ Close this dialog box when download completes



IMPORT / EXPORT

IMPORT

File*:

Password*:

EXPORT

Password*: ********

Confirm Password*: ********

- Navigate to the **Import / Export** screen.
- On the IMPORT / EXPORT screen, from the EXPORT section, in the Password field, enter your **Import / Export Password**.

Note: Import / Export passwords must be unique, are case sensitive, may have 6-32 alphanumeric characters, and may include underscores and dashes but not spaces.

- In the Confirm Password field, re-enter your **Import / Export Password**.
- Click **Export**.
- A system window appears. Click **Save** and the Save As screen appears.
- Navigate to an appropriate directory in your file system for saving the Export configuration file, and then click **Save**.
- When downloaded, the Download complete screen appears.
- Click **Close** and the IMPORT / EXPORT screen refreshes.

Determine if Multiple Systems are in Same Security World

To determine if two or more systems are in the same Security World, from the General Info screen, verify that each of the Security World ID names match. You may also determine this from the CLI start up screen, or by using the show hsm security-world-id or show general commands.

Determine if Admin Card is Part of a Security World

Users may check if the Admin card is part of the current Security World by using the hsm card checkpp command on the CLI. If the Admin card is not in the Security World, the CLI returns a message about the card not being recognized.

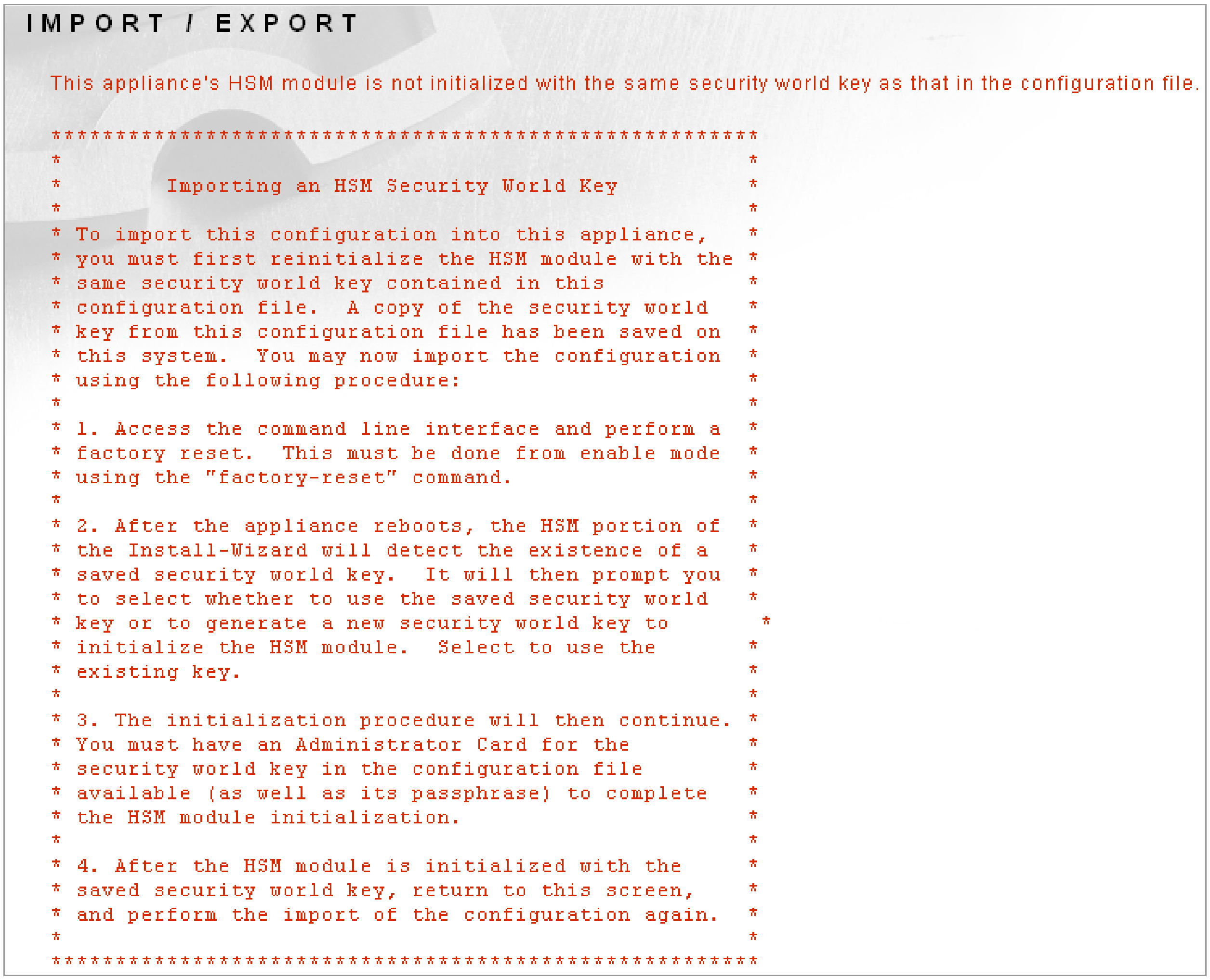
Import Same Configuration from HSM-enabled System to Another

Administrators may import a configuration from an HSM-enabled system (source is HSM-enabled system) to another HSM-enabled system (target also is HSM-enabled system) following the steps outlined in the earlier section entitled Export System Configuration.

However, if the HSM modules on each of the systems were initialized with a different Security World Key, then there will be extra steps involved (as mentioned earlier in Import or Export Configurations with Various System Versions section and detailed below in the HSM Import Error Message section).

Import Existing Configuration from HSM-enabled System to Another Initialized with Different Security World Key

When attempting to import an existing configuration from one HSM-enabled system (source is HSM-enabled system) to another (target is HSM-enabled system) and the target's HSM module was initialized with a different Security World Key than the source's, the initial import will fail and the following message appears:



This appliance's HSM module is not initialized with the same security world key as that in the configuration file.

```
*******************************************************
*                                                     *
*         Importing an HSM Security World Key         *
*                                                     *
* To import this configuration into this appliance,   *
* you must first reinitialize the HSM module with the *
* same security world key contained in this           *
* configuration file.  A copy of the security world   *
* key from this configuration file has been saved on  *
* this system.  You may now import the configuration  *
* using the following procedure:                      *
*                                                     *
* 1. Access the command line interface and perform a  *
* factory reset.  This must be done from enable mode  *
* using the "factory-reset" command.                  *
*                                                     *
* 2. After the appliance reboots, the HSM portion of  *
* the Install-Wizard will detect the existence of a   *
* saved security world key.  It will then prompt you  *
* to select whether to use the saved security world   *
* key or to generate a new security world key to       *
* initialize the HSM module.  Select to use the       *
* existing key.                                       *
*                                                     *
* 3. The initialization procedure will then continue. *
* You must have an Administrator Card for the         *
* security world key in the configuration file        *
* available (as well as its passphrase) to complete   *
* the HSM module initialization.                      *
*                                                     *
* 4. After the HSM module is initialized with the     *
* saved security world key, return to this screen,    *
* and perform the import of the configuration again.  *
*                                                     *
*******************************************************
```

Figure 4: HSM Import Error Message.

Note: After the import initially fails, the user must follow the instructions shown in the HSM Import Error Message section to successfully import the configuration including the new Security World:

1. Run the ***system config factory-reset*** command from the CLI enable mode. (When prompted, choose not to save the existing Security World - the HSM will be initialized after reboot with the new Security World key from the import .fsx file.)
2. After the system reboots, enter the CLI and complete the installation wizard. When populating the HSM module section of the Installation Wizard, the CLI will prompt the user whether to generate a new Security World Key or to use a saved one (from the configuration file that previously failed to import). Choose to use the saved one.
3. .The HSM module initialization procedure will then continue, during which the user must provide an Administrator card for the Security World Key in the configuration file (i.e. for the source system) and its passphrase. The user should then return to the product Import/Export screen and attempt to import the configuration file again.

Warning: The ***system config factory-reset*** command will delete all configuration data from the system including all policies, keys, users, groups, ACLs and Roles.

To review: the steps to perform this operation are:

- From the product **Import/Export** screen, on the HSM-enabled system (target), import the .fsx file created on the source system (this should fail initially with the error message shown above).
- From the CLI, switch to ***enable*** mode.
- Run the ***system config factory-reset*** command and select **Yes** when prompted to delete the existing Security World.

Note: When using the ***system config factory-reset*** command with an HSM-enabled system, the HSM security world will be deleted. The system will sense this during reboot and the user will be prompted to re-initialize the HSM on the CLI. With the serial connector attached to the system, cycle through the Forum™ Installation Wizard once again to enter your network configuration.

- Confirm that the Smart Card Reader is attached to the target HSM-enabled or FIPS-certified system.
- Access the CLI.
- The Forum Systems Installation Wizard starts.
- When presented with the choice: "Would you like to initialize the module with", reply by typing ***1*** for the option "The existing Security World Key using its corresponding Administrator Cards." and then press **<enter>**.
- Follow the onscreen prompts to complete the Installation Wizard (You will need an Administrator Card and its associated password for the Security World Key in the configuration file you are attempting to load to complete initialization of the HSM module).
- Return to the **Import/Export** screen and attempt to import the configuration file again.

Note: For more information, refer to the Initialize HSM on the CLI for the First Time chapter of the *Forum Systems Sentry™ Version 8.1 HSM Quick Start Guide*.

INDEX